# Skript: Vinzenz Schaller, Mathematikproseminar, HS 2016

# Quadratic reciprocity - Quadratisches Reziprozitätsgesetz

Das Quadratisches Reziprozitätsgesetz behandelt die eine allgemeinere Frage; 'Wann ist m $\in \mathbb{Z}$ ein Quadrat modul p?' D.h. Für welches m kann man ein x finden s.d. $x^2 = m, \text{mod. p}$ gilt? Um diese Frage zu beantworten betrachten wir zuerst die Definition des Legendre Symbols und bekommen mit dem Lemma und dem Gesetzt der quadratischen Reziprozität zwei Werkzeuge an die Hand, welches uns zeigt, wie mit dem Legendre Symbol umzugehen ist, s.d. die Frage abschliessend beantwortet werden kann.

**Definition des Legendre Symbol $\left(\frac{m}{p}\right)$, Sei $m \in \mathbb{Z}$ und p eine ungerade Primzahl.**

$$\left(\frac{m}{p}\right) = \begin{cases} 0 & \text{wenn p teilt m;} \\ +1 & \text{wenn p teilt nicht m und m ist ein Quadrat modulo p;} \\ -1 & \text{wenn p teilt nicht m und m ist kein Quadrat modulo p.} \end{cases}$$

**Primzahlenzerlegung beim Legendre Symbol**

$$\left(\frac{mn}{p}\right) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right), \text{ für } m, n \in \mathbb{Z}, \text{ p eine ungerade Primzahl.}$$

**Beweis:** Wir benutzen den Fakt, dass die Gruppe der Quadrate von $\mathbb{F}_p^\times$ als Untergruppe von $\mathbb{F}_p^\times$ den Index zwei hat. D.h. dass es nur zwei Nebenklassen in $\mathbb{F}_p^\times$ gibt. Dann haben wir: Seien $m, n \in \mathbb{F}_p^\times$. Sei Q die Gruppe der quadratischen Reste in $\mathbb{F}_p^\times$. Dann gilt:

$$[\mathbb{F}_p^\times : Q] = \frac{\text{ord } \mathbb{F}_p^\times}{\text{ord } G} = \frac{p-1}{\frac{p-1}{2}} = 2. \Rightarrow \mathbb{F}_p^\times = Q \dot{\vee} gQ, g \in \mathbb{F}_p^\times \backslash Q.$$

Wenn $\left(\frac{mn}{p}\right) = 0$, dann ist p ein Teiler des Produkts aus m und n, i.e. p ist ein Teiler von m oder n. Dies würde dann bedeuten, dass das entsprechende Legendresymbol gleich Null ist. Wenn also:

- $p|m \rightarrow \left(\frac{m}{p}\right) * \left(\frac{n}{p}\right) = 0 * \left(\frac{n}{p}\right) = 0 = \left(\frac{mn}{p}\right)\checkmark$
- $p|n \rightarrow \left(\frac{m}{p}\right) * \left(\frac{n}{p}\right) = \left(\frac{m}{p}\right) * 0 = 0 = \left(\frac{mn}{p}\right)\checkmark$

**Fallunterscheidung:** Wir unterscheiden nach $m, n \in Q$, $m \in Q, n \notin Q$ und $m, n \notin Q$.

Im ersten Fall gilt, dass $mn \in Q$, da Q eine Gruppe ist. Ansonsten gilt, dass $p|m, p|n \to p|m * n$. Daher gilt: $\left(\frac{mn}{p}\right) = 1$, und $\left(\frac{m}{p}\right) * \left(\frac{n}{p}\right) = 1 * 1 = 1$.✓ Für den zweiten Fall gilt: Angenommen $m * n \in Q$. Dann wäre $n \in m^{-1}Q = Q$.↯ Daher $m * n \notin Q$, und analog zu oben $\left(\frac{mn}{p}\right) = -1 = \left(\frac{m}{p}\right) * \left(\frac{n}{p}\right)$.✓ Im letzen Fall gilt: Angenommen $m * n \in Q$. Da $\mathbb{F}_p^\times = Q \dot\vee gQ, \forall g \in \mathbb{F}_p^\times \backslash Q : mQ = nQ$. $m1 = m \in mQ \to \exists g \in Q : m = ng$ mod. p. Also $n^{-1}m = g$ mod. p. Somit: $n^{-1} \notin Q$, ansonsten wäre $g \notin Q$, nach dem 2.ten Fall. Daher $n^{-1}Q = mQ. \to mnQ = Q \to mn \in Q$.↯ Also gilt $m * n \in Q$, und ausserdem $p \not| m$, $p \not| n \to p \not| n * m. \Rightarrow \left(\frac{mn}{p}\right) = +1 = (-1)(-1) = \left(\frac{m}{p}\right)\left(\frac{n}{p}\right)$. ✓ □

**Lemma 2.2.1**

$$\text{Für } n \in \mathbb{Z} : n^{(p-1)/2} \equiv \left(\frac{n}{p}\right), (\text{mod.} p).$$

**Beweis von Lemma 2.2.1** Das Resultat ist trivial, wenn n ein Vielfaches von p ist. Daher nehmen wir an, dass n nicht ein Vielfaches von p ist. Dann gilt nach Fermats Theorem: $n^{p-1} \equiv 1(\text{mod.} p)$, i.e. $n^{\frac{p-1}{2}} \equiv \pm 1(\text{mod.} p)$. Wenn nun n ein Quadrat modulo p ist, $n \equiv m^2$ (mod.) p, dann ist wieder durch Fermats Theorem: $n^{\frac{p-1}{2}} \equiv m^{p-1} \equiv 1(\text{mod.} p)$ Da $\mathbb{F}_p$ ein Körper ist, hat die Gleichung $x^{\frac{p-1}{2}} = 1$ höchstens $\frac{p-1}{2}$ Lösungen in $\mathbb{F}_p$. Da wir aber erst gerade geprüft haben, dass jedes Quadrat in $\mathbb{F}_p^\times$ eine Lösung darstellt, und es gibt $\frac{p-1}{2}$ solche Quadrate gilt mit anderen Worten, dass die Lösungsmenge von $x^{\frac{p-1}{2}} = 1$ genau die Menge von Quadraten in $\mathbb{F}_p^\times$ ist. □

**Theorom 2.2.2: Quadratisches Reziprozitätsgesetz** Sei p eine ungerade Primzahl, dann gilt:

(1) $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$;

(2) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$;

(3) Oder wenn q eine ungerade Primzahl ist, q ≠ p: $\left(\frac{q}{p}\right) = (-1)^{((p-1)(q-1))/4}\left(\frac{p}{q}\right)$.

**Beweis von Theorom 2.2.2: Ad 1) und ad 2)**

Ad 1 Dies ist eine reine Umformulierung des Theorems 2.1.7 von Fermat und Euler.

Erster Fall: Wir haben $(\frac{-1}{p}) = -1$ und somit ist -1 kein quadratischer Rest. Daher $p \not\equiv 1$ (mod. 4). (c.f.2.1.7) Somit gilt, dass $\frac{p-1}{2}$ ungerade ist, weil sonst $p \equiv 1$ (mod. 4)$\rightarrow (-1)^{\frac{p-1}{2}} = -1$.✓ Für den Fall, dass $-1$ ein Quadrat ist, gilt, dass $p \equiv 1$ (mod. 4) (c.f. 2.1.7.). Somit ist $\frac{p-1}{2}$ gerade, weil sonst $p \not\equiv 1$ (mod. 4). $\rightarrow (-1)^{\frac{p-1}{2}} = +1$. ✓

Ad 2 $\forall k \in \mathbb{Z}$ gibt es eine eindeutige ganze Zahl $r \in [-p/2; p/2]$ s.d. $k \equiv r(\text{mod}.p)$. Wir nennen dieses r das minimale Residue von k. Nun berechnen wir die minimalen Residue von $\frac{p-1}{2}$ Zahlen, genauer von 2,4,6, ..., p-1.

- Angenommen $p \equiv 1(\text{mod}.4)$. Dann erhalten wir: 2,4,6,8, ..., $\frac{p+3}{2}$, $\frac{p+1}{2}$, $+\frac{p-1}{2}$, $-\frac{p-3}{2}$, $-\frac{p-7}{2}$, $-\frac{p-9}{2}$, ...,-5,-3, -1 als minimale Residuen.
  - Beachte, dass wir im Absolutbetrag genau eine Permutation der $\frac{p-1}{2}$ Zahlen 1,2,3,4,5,6,7,8, ..., $\frac{p-1}{2}$ erhalten. Desweiteren haben $\frac{p-1}{4}$ von den minimalen Residuen ein negatives Vorzeichen. Durch die Multiplikation aller minimalen Residuen erhalten wir also:
    $(-1)^{\frac{p-1}{4}} \prod_{j=1}^{(p-1)/2} \equiv \prod_{j=1}^{(p-1)/2}(2j)$ (mod. p) $\equiv 2^{\frac{p-1}{2}} \prod_{j=1}^{(p-1)/2}(j)$ (mod. p).
    Streichen wir nun $\prod_{j=1}^{(p-1)/2}(j)$, erhalten wir: $2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{4}} \equiv (-1)^{\frac{p^2-1}{8}}$ (mod. p).
- Für $p \equiv 3$ (mod. 4) gehen wir analog vor, ausser dass wir nun $\frac{p+1}{4}$ minimale Residuen mit negativem Vorzeichen haben, wodurch nach einer ähnlichen Rechnung wieder folgt: $(\frac{2}{p}) = (-1)^{\frac{p+1}{4}} = (-1)^{\frac{p^2-1}{8}}$. □

**Lösungen zu den Übungen von 2.2. Quadratisches Reziprozitätsgesetz**

Aufgabe 1: Sei p eine ungerade Primzahl.
zz: $(p^2-1)$ ist durch 8 teilbar, i.e. $8|(p^2-1)$.
Beweis: $(p^2-1) = (p-1)*(p+1)$. Und da p ungerade ist, ist sowohl $(p-1)$, als auch $(p+1)$ eine gerade Zahl. Es gilt nicht nur das, sondern des weiteren, dass $(p-1)$ und $(p+1)$ gerade Zahlen sind, die direkt nebeneinander sind, i.e. eine davon ist durch 2 teilbar, und die andere ist durch 4 teilbar.
Sei nun $4|(p-1)$ und $2|(p+1)$. Dann definieren wir $c_1 := \frac{p-1}{4}$ und $c_2 := \frac{p+1}{2}$. Dann haben wir:

$$\begin{aligned}(p^2-1) &= (4*c_1)*(2*c_2) &= 4*c_1*2*c_2\\ &= 8*c_1*c_2 &= 8*(c_1*c_2).\text{qed}\end{aligned}$$

Aufgabe 2: Zeige, dass es $\frac{p-1}{2}$ Quadrate in $\mathbb{F}_p^\times$ gibt.
Beweis: Wir zeigen, dass $\phi : \mathbb{F}_p^\times \to \mathbb{F}_p^\times, x \mapsto x^2$ ein Gruppenhomomorphismus ist, und betrachten danach seinen Kern. $\phi$ ist ein Homomorphismus;

$$\begin{aligned} \phi(x*y) &= (x*y)^2 &&= (x*y)*(x*y) \\ &= x*x*y*y &&= x^2*y^2 \\ &&&= \phi(x)*\phi(y), \forall x,y \in \mathbb{F}_p^\times \checkmark \end{aligned}$$

Der Kern von $\phi$ ist: $\ker\phi = \{x \in \mathbb{F}_p^\times | \phi(x) = 1\}$ i.e.
$\phi(x) = 1 \leftrightarrow x^2 - 1 = 0 \leftrightarrow (x+1)*(x-1) = 0 \leftrightarrow x = \pm 1$ ,(mod. p). ✓
$\Rightarrow \ker\phi = \{\pm 1\}$. Mit der Theorem der Isomorphie[1] gilt für $\phi : G \to H$, dass $\frac{G}{\ker\phi} \cong$ im $\phi$. Bei uns ist nun G, $\ker\phi$ und im $\phi$ endlich s.d. $\frac{|G|}{|\ker\phi|} = |\text{im}\phi| = \{y \in \mathbb{F}_p^\times : y = x^2,$ für ein $x \in \mathbb{F}_p^\times\}$. Und somit haben wir für $\frac{|\mathbb{F}_p^\times|}{|\{\pm 1\}|} = \frac{p-1}{2}$. □

[1] Noether I

## Sums of 4 squares - Summen von 4 Quadraten

Das Ziel dieses Unterkapitels ist der Beweis des klassischen Theorems, das von Jacobi stammt, was folgendes aussagt.

**Theorom 2.3.1** Sei n eine positive ungerade ganze Zahl. Dann ist $r_4(n) = 8 \sum_{d|n} d$.

**Lemma 2.3.2 mit Beweis** Für den Beweis des Theorems 2.3.1 brauchen wir unteranderem das Lemma 2.3.2, $\forall n \in \mathbb{N} : r_4(2n) = r_4(4n)$, was ich hier beispielhaft für die anderen Lemmas beweisen werde.

- Wenn $x_0^2 + x_1^2 + x_2^2 + x_3^2 = 4n = 4n + 0, x_i \in \mathbb{Z}$ sieht man durch die Reduktion mod. 4, dass entweder alle $x_i$ gerade sind, oder alle $x_i$ ungerade sind.

  – Es gilt $x_0^2 + x_1^2 + x_2^2 + x_3^2 = 4n = 4n + 0$ nämlich nur für den Fall, dass $\forall i = 0, 1, 2, 3 : x_i = 2k \rightarrow x_0^2 + x_1^2 + x_2^2 + x_3^2 = 4k_0^2 + 4k_1^2 + 4k_2^2 + 4k_3^2 = 4(k_0^2 + k_1^2 + k_2^2 + k_3^2) = 4n + 0$, und für den Fall, dass $\forall i = 0, 1, 2, 3 : x_i = 2k + 1 \rightarrow x_0^2 + x_1^2 + x_2^2 + x_3^2 = 4k_0^2 + 4k_0 + 1 + \cdots + 4k_3^2 + 4k_3 + 1 = 4(k_0^2 + k_0 + \cdots + k_3^2 + k_3) = 4n + 0$. ✓ Aber wenn 1,2 oder 3 $x_i$ gerade und damit 3,2 oder 1 $x_i$ ungerade sind, dann kann die 4 nicht aus allen Termen heraus faktorisiert werden, weil die 1 aus der ungeraden $x_i$ dann 1,2 oder 3 mal vorkommen, und so nach der Faktorisierung mit 4 das Ergebnis gleich $4n + 1, 4n + 2$ oder $4n + 3$ ist, was ein Widerspruch zur Annahme darstellt.

  Somit bildet der Variablenwechsel ...

$$y_0 = \frac{x_0 - x_1}{2}, y_1 = \frac{x_0 + x_1}{2}, y_2 = \frac{x_2 - x_3}{2}, y_3 = \frac{x_2 + x_3}{2}$$

  (mit den Inversen $x_0 = y_0 + y_1, x_1 = y_1 - y_0, x_2 = y_1 + y_3, x_3 = y_3 - y_2$)

- ... die ganzzahlige Lösung $x_0^2 + x_1^2 + x_2^2 + x_3^2 = 4n$ auf eine ganzzahlige Lösung von $y_0^2 + y_1^2 + y_2^2 + y_3^2 = 2n$ ab, und stellt somit eine Bijektion zwischen den zwei Mengen her.

  Beweis der Bijektivität: Sei $\phi : \{$Lösungen $(x_0, x_1, x_2, x_3)$ von $x_0^2 + x_1^2 + x_2^2 + x_3^2 = 4n\}$ $\rightarrow \{$Lösungen $(y_0, y_1, y_2, y_3)$ von $y_0^2 + y_1^2 + y_2^2 + y_3^2 = 2n\}$

wohldefiniert: Sei $(x_0, x_1, x_2, x_3)$ Lösung von $(x_0)^2 + (x_1)^2 + (x_2)^2 + (x_3)^2 = 4n$. Dann ist $\phi(x_0, x_1, x_2, x_3) = (y_0, y_1, y_2, y_3)$ Lösung von $(y_0)^2 + (y_1)^2 + (y_2)^2 + (y_3)^2 = 2n$.

$$(y_0)^2+(y_1)^2+(y_2)^2+(y_3)^2 = (\frac{x_0-x_1}{2})^2+(\frac{x_0+x_1}{2})^2+(\frac{x_2-x_3}{2})^2+(\frac{x_2+x_3}{2})^2$$
$$= \frac{x_0^2}{4} - \cancel{\frac{x_0x_1}{2}} + \frac{x_1^2}{4} + \frac{x_0^2}{4} + \cancel{\frac{x_0x_1}{2}} + \cdots = \frac{x_0^2}{2}+\frac{x_1^2}{2}+\frac{x_2^2}{2}+\frac{x_3^2}{2}$$
$$= \frac{1}{2}((x_0)^2+(x_1)^2+(x_2)^2+(x_3)^2) = \frac{1}{2}*4n = 2n.\checkmark$$

injektiv: Sei $\phi(x_0,x_1,x_2,x_3) = \phi(x_0',x_1',x_2',x_3')$. Dann gilt: $\frac{x_0-x_1}{2} = \frac{x_0'-x_1'}{2}; \frac{x_0+x_1}{2} = \frac{x_0'+x_1'}{2}; \ldots$ und durch die Addition und Subkration der Terme erhalten wir die gesuchten Identitäten.✓

surjektiv: Sei $(y_0,y_1,y_2,y_3)$ Lösung von $(y_0)^2+(y_1)^2+(y_2)^2+(y_3)^2 = 2n$. Dann gilt: $(x_0,x_1,x_2,x_3) := (y_0+y_1, y_1-y_0, y_2+y_3, y_3-y_2)$ löst $x_0^2+x_1^2+x_2^2+x_3^2 = 4n$.

$$(x_0)^2+(x_1)^2+(x_2)^2+(x_3)^2 = (y_0+y_1)^2+(y_1-y_0)^2+(y_2+y_3)^2+(y_3-y_2)^2$$
$$= y_0^2+2*y_0y_1+y_1^2+\cdots = 2y_0^2+2y_1^2+2y_2^2+y_3^2$$
$$= 2(y_0^2+y_1^2+y_2^2+y_3^2) = 2*2n = 4n.$$

Und $\phi(x_0,x_1,x_2,x_3) = (\frac{(y_0+y_1)-(y_1-y_0)}{2},\ldots,\ldots,\ldots) = (y_0,y_1,y_2,y_3).\square$

**Beweis des Theorems 2.3.1** Der Beweis dieses Theorems beruht auf 3 Lemmas.

2.3.2 Lemma : Für alle $n \in \mathbb{N}$ : $r_4(2n) = r_4(4n)$.

2.3.3 Lemma : Für alle ungraden $n \in \mathbb{N}$ : $r_4(2n) = 3r_4(n)$.

2.3.4 Lemma : Für alle ungraden $n \in \mathbb{N}$ : $N_4(4n) = \sum_{d|n} d$.

Danach erfolgt der Beweis wie folgt:

- Behauptung: Für n ungerade erhalten wir $r_4(4n) = 16N_4(4n) + r_4(n)$. [2]

  In der Tat. Wenn $x_0^2+x_1^2+x_2^2+x_3^2 = 4n, x_i \in \mathbb{Z}$ (wie im Beweis von Lemma 2.3.2), dann sind entweder alle $x_i$ gerade oder alle $x_i$ sind ungerade. Im ersten Fall erhalten wir durch den Variablenwechsel ,$y_i = \frac{x_1}{2}$(weil $x_i$gerade), $i = 0,1,2,3$, eine Bijektion zwischen der Menge von geraden Lösungen von $x_0^2+x_1^2+x_2^2+x_3^2 = 4n$ und

[2] $N_k(n)$ ist die Anzahl von Darstellungen von n als eine Summe von k Quadraten, wobei nur positive ungeraden Zahlen verwendet werden, i.e. $N_k(n) = |\{(x_0,\ldots,x_{k-1}) \in \mathbb{N}^k : \sum_{i=0}^{k-1} x_i^2 = n; x_i \text{ ungerade}\}|$.

der Menge von Lösungen von $y_0^2 + y_1^2 + y_2^2 + y_3^2 = n$. Somit haben wir dann $r_4(n)$ solche Lösungen. Im zweiten Fall haben wir $16N_4(4n)$ Lösungen (Der Koeffizient 16 kommt von $2^4$ möglichen Ziehungen für das Vorzeichen von den $x_i$.) Dies beweist die Behauptung. Damit betrachten wir nun

$$\begin{aligned} 3r_4(n) &= r_4(2n) \text{ ,durch Lemma 2.3.3} \\ &= r_4(4n) \text{ ,durch Lemma 2.3.2} \\ &= 16N_4(4n) + r_4(n) \text{ ,durch die obere Behauptung} \\ &= 16(\sum_{d|n} d) + r_4(n) \text{ ,durch Lemma 2.3.4} \end{aligned}$$

- Durch das Kürzen erhalten wir nun die Behauptung von 2.3.1. □

**Lösungen zu den Übungen von 2.3. Die Summe von 4 Quadraten: Aufgabe 1** Überprüfe, dass der Beweis von Lemma 2.3.3. gegebene inverse Variablenwechsel Lösungen von $y_0^2 + y_1^2 + y_2^2 * y_3^2 = n$ auf Lösungen von $x_0^2 + x_1^2 + x_2^2 + x_3^2 = 2n$ abbildet, s.d. die entsprechenden Praritätsbedingungen erfüllt sind, i.e. zeige, dass $\phi$ wohldefiniert ist, und genau zwei $x_i$ gerade und ungerade sind. Beweis:

$\phi : \{(y_0, \ldots, y_3) : y_0^2 + \cdots + y_3^2 = n\} \to \{(x_0, \ldots, x_3) : x_0^2 + \cdots + x_3^2 = 2n\}$ ist wohldefiniert.

Sei $(y_0, \ldots, y_3)$ s.d. $y_0^2 + \cdots + y_3^2 = n$. Dann ist $\phi(y_0, \ldots, y_3) = (y_0 + y_1, y_1 - y_0, y_2 + y_3, y_3 - y_2) =: (x_0, \ldots, x_3)$ und wir erhalten

$$\begin{aligned} x_0^2 + \cdots + x_3^2 &= (y_0 + y_1) + (y_1 - y_0) + \ldots \\ &= y_0^2 + 2y_0y_1 + y_1^2 + y_1^2 - 2y_0y_1 + y_0^2 + \ldots \\ &= 2y_0^2 + 2y_1^2 + 2y_2^2 + 2y_3^2 \\ &= 2 * (y_0^2 + y_1^2 + y_2^2 + y_3^2) = 2n. \checkmark \end{aligned}$$

Für $(x_0, x_1, x_2, x_3) = \phi(y_0, y_1, y_2, y_3)$ sind immer genau zwei $x_i$ gerade und zwei sind ungerade.

Da n nach Annahme ungerade ist, und $y_0^2 + \cdots + y_3^2 = n$ gilt, dass $y_0^2 + \cdots + y_3^2 = 1$, mod. 2. Somit sind exakt 1 oder 3 der $y_i$ ungerade;

- Wenn 3 $y_i$ ungerade sind, dann gilt o.B.d.A. $y_0, y_1, y_2$ ungerade und $y_3$ gerade. Was zur Folge hat, dass: $x_0 = y_0 + y_1$ gerade, $x_1 = y_1 - y_0$ gerade, $x_2 = y_2 + y_3$ ungerade, $x_3 = y_2 - y_3$ ungerade.

– Wenn 1 $y_i$ ungerade ist, dann gilt o.B.d.A. $y_0$ ungerade und $y_1, y_2, y_3$ gerade. Was zur Folge hat, dass: $x_0 = y_0 + y_1$ gerade, $x_1 = y_1 - y_0$ ungerade, $x_2 = y_2 + y_3$ gerade und $y_3 - y_2$ gerade. $\square$